MATHEMATICS

ON SPLITTING PROPERTIES OF PRIMES BY MEANS OF ARTIN CONDUCTORS

BY

ROBERT W. VAN DER WAALL

(Communicated by Prof. T. A. Springer at the meeting of September 29, 1973)

Introduction

In a previous paper, see [1], we dealt with the following situation: Let p be an odd prime, and suppose that $X^p - a \in \mathbf{Z}[X]$ is an irreducible polynomial over $\mathbf{Q}$, the field of the rational numbers. We studied the decomposition behaviour of the prime p and of the primes dividing the integer a in the field $\mathbf{Q}(\sqrt[p]{a})$, where moreover $p \nmid a$. The results of [1] were obtained by means of the so-called Artin-conductors. The whole problem was a global problem, and as Professor Helmut Koch from East-Berlin pointed out to me, it is also possible to obtain the results by localization methods à la Hensel.

Later I found out that in the book Integral Bases by W. E. H. Berwick, see [2], the same results were proved, however as an example of extremely hard arithmetical computations dealing with the determination of local bases for the integers of an algebraic number field.

However in my opinion my method circumvents all these arithmetical difficulties. In [2], the splitting of p in the field $\mathbf{Q}(\sqrt[p^h]{a})$ is considered too, where h is an integer, $\geqslant 2$. Notice: $X^{p^h} - a$ is irreducible over $\mathbf{Q}$ if and only if $X^p - a$ is irreducible over $\mathbf{Q}$, see [3], Satz 7, Seite 291.

It is the purpose of this paper to derive the splitting behaviour of p in $\mathbf{Q}(\sqrt[p^2]{a})$, $a \in \mathbf{Z}$, where a is not a p^{th}-power of an element of $\mathbf{Z}$, by means of a generalization of the methods used in [1].

In § 2 we just state what the results are for $\mathbf{Q}(\sqrt[p^h]{a})$, $h \geqslant 2$.

Notations

a	a rational integer not a p^{th}-power of some other rational integer, and such that $p \nmid a$.
p	a (positive) odd prime.
$\Delta_{T/S}$	the discriminant of the algebraic number field T relative to the subfield S.
$\mathfrak{f}_\chi = \mathfrak{f}_\chi(L/K)$	the conductor of the character χ, where χ is a character of Gal (L/K), when L/K is a finite Galois extension.

Further notation is adopted from [1].

Throughout in this paper we fix once and for all the roots $\sqrt[p^i]{a}$, such that $(\sqrt[p^i]{a})^p=\sqrt[p^{i-1}]{a}$.

In the paper [1] we presupposed that $\sqrt[p]{a}\in\mathbf{R}$, but this condition is in fact superfluous.

§ 1.

Let A_i be the ring of integers of $\mathbf{Q}(\sqrt[p^i]{a})$, let $\zeta=e^{2\pi i/p}$, let B_i be the ring of integers of $\mathbf{Q}(\zeta, \sqrt[p^i]{a})$.

$\mathfrak{P}_{i,j}$ are always prime ideals of B_j; $\mathfrak{p}_{i,j}$ are always prime ideals of A_j.

We prove the following

THEOREM 1:

(1) If $a^p\not\equiv a \pmod{p^2}$, then $pA_2=\mathfrak{p}_{1,2}^{p^2}$.

(2) If $a^p\equiv a \pmod{p^2}$, then $pA_1=\mathfrak{p}_{1,1}^{p-1}\,\mathfrak{p}_{2,1}$.

(3) We use the notation as under (2):
If $a^p\equiv a \pmod{p^2}$, but $a\not\equiv\sqrt[p]{a} \pmod{\mathfrak{p}_{2,1}^2}$, then

$$pA_2=\mathfrak{p}_{1,2}^{p(p-1)}\,\mathfrak{p}_{2,2}^{p}.$$

(4) We use the notation as under (2):
If $a\equiv\sqrt[p]{a} \pmod{\mathfrak{p}_{2,1}^2}$, then

$$pA_2=\mathfrak{p}_{1,2}^{p(p-1)}\,\mathfrak{p}_{2,2}^{p-1}\,\mathfrak{p}_{3,2}.$$

PROOF:

(1) In this case we have $pA_1=\mathfrak{p}_{1,1}^{p}$. See [1]. Look at the fig. 1. We have

$$[\mathbf{Q}(\sqrt[p]{a}):\mathbf{Q}]=[\mathbf{Q}(\sqrt[p^2]{a}):\mathbf{Q}(\sqrt[p]{a})]=[L:K]=[K:\mathbf{Q}(\zeta)]=p,$$

and

$$[\mathbf{Q}(\zeta):\mathbf{Q}]=[K:\mathbf{Q}(\sqrt[p]{a})]=[L:\mathbf{Q}(\sqrt[p^2]{a})]=p-1.$$

The ring of integers of $\mathbf{Q}(\zeta)$ is $\mathbf{Z}[\zeta]$. Let $\pi=(1-\zeta)$ then $p\mathbf{Z}[\zeta]=\pi^{p-1}$. π is a prime ideal of $\mathbf{Z}[\zeta]$. Since $K/\mathbf{Q}(\zeta)$ is a Galois extension, it follows now from $pA_1=\mathfrak{p}_{1,1}^{p}$ that $\mathfrak{p}_{1,1}B_1=\mathfrak{P}_{1,1}^{p-1}$. Hence the ideal $\mathfrak{p}_{1,1}$ is ramified in the Galois closure of the extension $\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}(\sqrt[p]{a})$, i.e. $L/\mathbf{Q}(\sqrt[p]{a})$. Next we show

$$\begin{tikzcd}
\mathbf{Q}(\zeta) \arrow[r, dash] \arrow[d, dash] & K=\mathbf{Q}(\zeta, \sqrt[p]{a}) \arrow[r, dash] \arrow[d, dash] & L=\mathbf{Q}(\zeta, \sqrt[p^2]{a}) \arrow[d, dash] \\
\mathbf{Q} \arrow[r, dash] & \mathbf{Q}(\sqrt[p]{a}) \arrow[r, dash] & \mathbf{Q}(\sqrt[p^2]{a})
\end{tikzcd}$$

Fig. 1.

that the congruence $X^p \equiv {}^p\sqrt{a} \pmod{\mathfrak{P}_{1,1}^{p^2}}$ has no solution in B_1. (Notice that $\pi B_1 = \mathfrak{P}_{1,1}^p$). Suppose the congruence would have a solution x in B_1. Take $s \in B_1$ such that $x = {}^p\sqrt{a} + s$. Then:

$${}^p\sqrt{a} \equiv ({}^p\sqrt{a}+s)^p = a + \binom{p}{1} ({}^p\sqrt{a})^{p-1} s + \ldots + \binom{p}{p-1} ({}^p\sqrt{a}) s^{p-1} + s^p \pmod{\mathfrak{P}_{1,1}^{p^2}}.$$

Since $a^p - a = (a - {}^p\sqrt{a})(a - \zeta\, {}^p\sqrt{a}) \ldots (a - \zeta^{p-1}\, {}^p\sqrt{a})$ it follows that $\mathfrak{P}_{1,1}$ divides $a - \zeta^j\, {}^p\sqrt{a}$ for some $j \pmod p$. Since $a - {}^p\sqrt{a} = a - \zeta^j\, {}^p\sqrt{a} + (1 - \zeta^{-j})\zeta^j\, {}^p\sqrt{a}$, and $\pi = (1-\zeta)$ it follows that $\mathfrak{P}_{1,1}$ divides $a - {}^p\sqrt{a}$. Hence $\mathfrak{P}_{1,1} | s^p$, so $\mathfrak{P}_{1,1} | s$. From this we see that

$${}^p\sqrt{a} - a \equiv 0 \pmod{\mathfrak{P}_{1,1}^p}.$$

Since $\mathfrak{P}_{1,1}$ is totally ramified over $\mathbf{Q}$, it follows by taking norms that

$$\mathfrak{p}_{1,1}^p | ({}^p\sqrt{a} - a)^{p-1}$$

whence

$$\mathfrak{p}_{1,1}^2 | {}^p\sqrt{a} - a.$$

Now

$$N_{\mathbf{Q}({}^p\sqrt{a})/\mathbf{Q}}\ \mathfrak{p}_{1,1}^2 | N_{\mathbf{Q}({}^p\sqrt{a})/\mathbf{Q}}\ ({}^p\sqrt{a} - a),$$

so

$$p^2 | a - a^p,$$

what is not true in this case.

Therefore the insolvability of the congruence mentioned above leads to the fact that $\mathfrak{P}_{1,1}$ ramifies totally in L; of course we used here again the fact that L/K is a Galois extension. But then it is clear that $pA_2 = \mathfrak{p}_{1,2}^{p^2}$.

(2) See [1].

(3) Since $a^p \equiv a \pmod{p^2}$ we have the situation of (2) namely $pA_1 = \mathfrak{p}_{1,1}^{p-1}\mathfrak{p}_{2,1}$. From [1] we know that

$$\pi B_1 = \mathfrak{P}_{1,1} \ldots \mathfrak{P}_{p-1,1}\mathfrak{P}_{p,1}.$$

Also in [1] we have seen that

$$\mathfrak{p}_{1,1}B_1 = \mathfrak{P}_{1,1} \ldots \mathfrak{P}_{p-1,1} \text{ and } \mathfrak{p}_{2,1}B_1 = \mathfrak{P}_{p,1}^{p-1}.$$

Since $L/\mathbf{Q}({}^p\sqrt{a})$ is the Galois closure of the extension $\mathbf{Q}({}^{p^2}\sqrt{a})/\mathbf{Q}({}^p\sqrt{a})$ it follows from the ramification of $\mathfrak{p}_{2,1}$ in B_1, that $\mathfrak{p}_{2,1}$ is ramified in $\mathbf{Q}({}^{p^2}\sqrt{a})$, but what is the actual decomposition of $\mathfrak{p}_{2,1}$ in $\mathbf{Q}({}^{p^2}\sqrt{a})$?

We investigate the congruence

$$X^p \equiv {}^p\sqrt{a} \pmod{\mathfrak{P}_{p,1}^p}.$$

(Notice that $\mathfrak{P}_{p,1} | \pi$ but $\mathfrak{P}_{p,1}^2 \nmid \pi$). Suppose that the congruence has a solution in B_1, say x. Let $x = {}^p\sqrt{a} + s$, then $s \in B_1$. Since $\mathfrak{P}_{p,1}^{p-1} | p$ and $\mathfrak{P}_{p,1} | s$, we derive along the lines of the proof of (1) that ${}^p\sqrt{a} \equiv a \pmod{\mathfrak{P}_{p,1}^p}$. By taking norms it follows that $\mathfrak{p}_{2,1}^p | ({}^p\sqrt{a} - a)^{p-1}$, hence that $\mathfrak{p}_{2,1}^2 | {}^p\sqrt{a} - a$, what is not true in this case (3).

Therefore, and by the fact that L/K is a Galois extension of degree p, we conclude that $\mathfrak{P}_{p,1}$ is totally ramified in L. Hence $\mathfrak{p}_{2,1}$ is totally ramified in L, with $\mathfrak{p}_{2,1}B_2=\mathfrak{P}_{p,2}^{p(p-1)}$. Hence

$$\mathfrak{p}_{2,1}A_2=\mathfrak{p}_{2,2}^{p}.$$

Or, equivalently,

$$\mathfrak{p}_{2,2}^{p}|p, \text{ but } \mathfrak{p}_{2,2}^{p+1}\nmid p,$$

where $\mathfrak{p}_{2,2}$ is the unique prime ideal of A_2 lying above $\mathfrak{p}_{2,1}$.

Next we have to decide whether $\mathfrak{p}_{1,1}$ is ramified in A_2 or not. In order to do this, we calculate some typical divisors of the relative discriminant $\Delta=\Delta_{\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}(\sqrt[p]{a})}$. Only the prime ideals of $\mathbf{Q}(\sqrt[p]{a})$ that ramify in $\mathbf{Q}(\sqrt[p^2]{a})$ divide Δ.

Now

$$\Delta|N_{\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}(\sqrt[p]{a})}\, f'(\sqrt[p^2]{a})A_1,$$

where $f(X)=X^p-\sqrt[p]{a}\in\mathbf{Q}(\sqrt[p]{a})[X]$.

Hence:

$$\Delta|p^p(\sqrt[p]{a})^{p-1}A_1.$$

Since $p\nmid a$, we have $\mathfrak{p}_{2,1}\nmid\sqrt[p]{a}$.

Hence

$$\Delta|\mathfrak{p}_{1,1}^{p(p-1)}\,\mathfrak{p}_{2,1}^{p}\,J,$$

where J is an ideal of A_1, relatively prime to both $\mathfrak{p}_{1,1}$ and $\mathfrak{p}_{2,1}$.

Since $\mathfrak{p}_{2,1}A_2=\mathfrak{p}_{2,2}^{p}$, it follows then from ramification theory that $\mathfrak{p}_{2,1}^{p}$ divides Δ "exactly" i.e. $\mathfrak{p}_{2,1}^{p}|\Delta$, but $\mathfrak{p}_{2,1}^{p+1}\nmid\Delta$.

Next we use the following lemma, whose proof will be given in the Appendix:

LEMMA 1: In the cases (3) and (4) of Theorem 1 we have:

$$p^{p^2-2}|N_{\mathbf{Q}(\sqrt[p]{a})/\mathbf{Q}}\,\Delta.$$

From the lemma 1 we conclude that the prime ideal $\mathfrak{p}_{1,1}$ must ramify in $\mathbf{Q}(\sqrt[p^2]{a})$. Since $\mathfrak{p}_{1,1}$ is decomposed completely in B_1 and since $L/\mathbf{Q}(\sqrt[p]{a})$ and L/K are Galois extensions, all the $\mathfrak{P}_{1,1},\ldots,\mathfrak{P}_{p-1,1}$ must ramify totally in B_2 (notice again that $[L:K]=p$). Hence we have $\mathfrak{p}_{1,1}A_2=\mathfrak{p}_{1,2}^{p}$. Moreover we see that $\mathfrak{p}_{1,2}$ is decomposed completely in B_2 and that $\mathfrak{p}_{2,2}$ is fully and tamely ramified in B_2. For we have $\mathfrak{P}_{p,1}B_2=\mathfrak{P}_{p,2}^{p}$ and $\mathfrak{p}_{2,2}B_2=\mathfrak{P}_{p,2}^{p-1}$.

(4) Since $a\equiv\sqrt[p]{a} \pmod{\mathfrak{p}_{2,1}^{2}}$ we have $a^p\equiv a \pmod{p^2}$ by taking the appropriate norm. Hence, with the notation of (3), we find $a\equiv\sqrt[p]{a}$ $(\mathrm{mod}\ \mathfrak{P}_{p,1}^{2(p-1)})$. Since $p+1<2p-2$ we have: $a\equiv\sqrt[p]{a}$ $(\mathrm{mod}\ \mathfrak{P}_{p,1}^{p+1})$. But this is precisely the condition that $\mathfrak{P}_{p,1}$ is decomposed completely in B_2. Now $\mathfrak{p}_{2,1}$ is ramified in L, as it is in K. Since $L/\mathbf{Q}(\sqrt[p]{a})$ is the Galois closure of $\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}(\sqrt[p]{a})$ it follows now (by the complete decomposition of $\mathfrak{P}_{p,1}$

in B_2) that $\mathfrak{p}_{2,1}$ is ramified in $\mathbf{Q}(\sqrt[p^2]{a})$, however such that

$$\mathfrak{p}_{2,1}A_2 = \mathfrak{q}_{1,2}^{e_1} \dots \mathfrak{q}_{r,2}^{e_r},$$

with the $\mathfrak{q}_{j,2}$ prime ideals of A_2, and such that $r \geqslant 2$. Moreover $\sum_{i=1}^{r} e_i = p$. (Notice that the residue degree of every $\mathfrak{q}_{j,2}$ over $\mathfrak{p}_{2,1}$ is equal to 1, by looking at the decomposition $\mathfrak{p}_{2,1}B_1 = \mathfrak{P}_{p,1}^{p-1}$ and $\mathfrak{P}_{p,1}B_2 = \mathfrak{P}_{1,2} \dots \mathfrak{P}_{p,2}$).

Now Gal $(L/\mathbf{Q}(\sqrt[p]{a}))$ is isomorphic to Gal $(K/\mathbf{Q})$. Let χ be the unique faithful simple character of Gal $(L/\mathbf{Q}(\sqrt[p]{a}))$. Then $\mathfrak{f}_\chi$ is an integral ideal of $\mathbf{Q}(\sqrt[p]{a})$. Just as we did it in the paper [1] we conclude that

$$\mathfrak{p}_{2,1}^{p-2} \text{ divides } \mathfrak{f}_\chi = \Delta_{\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}(\sqrt[p]{a})} \text{ "exactly".}$$

From this we derive

$$r=2, \; e_1 = 1 \text{ or } e_1 = p-1 \text{ and } e_2 = p - e_1.$$

Now using the lemma 1 and by what we have said in (3) it follows that $\mathfrak{p}_{1,1}A_2 = \mathfrak{p}_{1,2}^{p}$.

The proof of Theorem 1 is now complete. q.e.d.

Corollary 1:

(i) If $a^p \equiv a \pmod{p^3}$, then case (4) of Theorem 1 holds.

(ii) If $a^p \not\equiv a \pmod{p^3}$ but $a^p \equiv a \pmod{p^2}$, then case (3) of Theorem 1 holds.

Proof: (i) We have

$$p^3 | a - a^p = (\sqrt[p]{a} - a)^p + \binom{p}{1} (\sqrt[p]{a} - a)^{p-1} a + \dots + \binom{p}{p-1} (\sqrt[p]{a} - a) a^{p-1}.$$

From the proof of Theorem 1 we easily derive that the prime ideal $\mathfrak{p}_{1,2}$ of A_1 divides $\sqrt[p]{a} - a$. But then (using that $pA_1 = \mathfrak{p}_{1,1}^{p-1}\, \mathfrak{p}_{1,2}$):

$$\mathfrak{p}_{1,2}^{3} | a - a^p \Rightarrow \mathfrak{p}_{1,2}^{3} | p(\sqrt[p]{a} - a) a^{p-1} \Rightarrow \mathfrak{p}_{1,2}^{2} | \sqrt[p]{a} - a.$$

Hence we are in case (4).

(ii) Suppose that (4) holds. Then $a \equiv \sqrt[p]{a} \pmod{\mathfrak{p}_{1,2}^2}$ and by taking norms we find $a^p \equiv a \pmod{p^2}$. We have in case (4) a complete decomposition of π into p different prime ideals $\mathfrak{P}_{1,1}, \dots, \mathfrak{P}_{p-1,1}, \mathfrak{P}_{p,1}$ of B_1. We adopt the notation from Theorem 1, case (3) and (4), namely $\mathfrak{p}_{1,2}B_1 = \mathfrak{P}_{p,1}^{p-1}$.

Now every such $\mathfrak{P}_{j,1}$ divides $\sqrt[p]{a} - a$. Hence we have

$$\sqrt[p]{a} \equiv a \pmod{\mathfrak{P}_{1,1} \dots \mathfrak{P}_{p-1,1} \mathfrak{P}_{p,1}^{2p-2}}.$$

Then

$$\begin{gathered} N_{K/\mathbf{Q}(\zeta)} (\mathfrak{P}_{1,1} \dots \mathfrak{P}_{p-1,1} \mathfrak{P}_{p,1}^{2p-2}) | N_{K/\mathbf{Q}(\zeta)} (\sqrt[p]{a} - a) \\ \pi^{3p-3} | a^p - a \\ p^{3p-3} | (a^p - a)^{p-1} \\ p^3 | a^p - a. \end{gathered}$$

And therefore the proof of the corollary is complete. q.e.d.

§ 2.

On account of the Theorem 1 and the Corollary 1 we have the following

THEOREM 2: Let $a^p \equiv a \pmod{p^j}$, and $a^p \not\equiv a \pmod{p^{j+1}}$, $j \geqslant 2$. Then, with the notations as in § 1, we have:
(i) If $2 \leqslant j \leqslant h$, then

$$pA_h = \mathfrak{p}_{1,h}^{\varphi(p^h)}\, \mathfrak{p}_{2,h}^{\varphi(p^{h-1})} \cdots \mathfrak{p}_{j-1,h}^{\varphi(p^{h-j+2})}\, \mathfrak{p}_{j,h}^{\varphi(p^{h-j+2})/(p-1)}.$$

(ii) If $j \geqslant h+1$, then

$$pA_h = \mathfrak{p}_{1,h}^{\varphi(p^h)}\, \mathfrak{p}_{2,h}^{\varphi(p^{h-1})} \cdots \mathfrak{p}_{h-1,h}^{\varphi(p^2)}\, \mathfrak{p}_{h,h}^{\varphi(p)}\, \mathfrak{p}_{h+1,h}.$$

(Here $\varphi(n)$ is Euler's totient function).

PROOF: We omit the proof because our calculations are at least as difficult as in [2], the cases $\mathbf{Q}(\sqrt[p]{a})$ and $\mathbf{Q}(\sqrt[p^2]{a})$ excepted.

APPENDIX

In this appendix we prove the lemma 1, which is the keystone of the proof of Theorem 1.

Let $\eta = \exp(2\pi i/p^2)$. Let L and K be as in the fig. 1. We will study the structure of $\mathrm{Gal}(L(\eta)/\mathbf{Q})$. It is easily seen that $\mathrm{Gal}(L(\eta)/\mathbf{Q}) = HA$, where H is cyclic of order p^2, H normal in HA, $H = \mathrm{Gal}(L(\eta)/\mathbf{Q}(\eta))$, $A \cong \mathrm{Aut}(H)$, $A = \mathrm{Gal}(L(\eta)/\mathbf{Q}(\sqrt[p^2]{a}))$, A is cyclic and of order $p(p-1)$. A acts in an obvious way on H. HA has $p(p-1)$ linear (simple) complex characters, p simple complex characters all of degree $p-1$, and precisely one simple complex character of degree $p(p-1)$. Call the latter character χ. This character χ is faithful, and is induced by some linear character ψ of H. Now take the trivial character λ_0 of A. A direct calculation shows that

$$\lambda_0^* = \chi_0 + \chi_p + \chi. \quad [\lambda_0^* \text{ is the character of } HA, \text{ induced by } \lambda_0]$$

Here χ_0 is the trivial character of HA, χ_p is the unique non-linear simple character of $\mathrm{Gal}(K/\mathbf{Q})$, (hence χ_p is also a character of HA, since $\mathrm{Gal}(K/\mathbf{Q})$ is a factor group of HA), and χ is just the character mentioned above.

Now the conductor-calculus! We have

$$\mathfrak{f}_{\chi_p}\, \mathfrak{f}_{\chi} = \Delta_{\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}},$$

since this is all what remains from the formula

$$\mathfrak{f}_{\chi_0+\chi_p+\chi} = \mathfrak{f}_{\chi_0}\mathfrak{f}_{\chi_p}\mathfrak{f}_{\chi} = \mathfrak{f}_{\chi_p}\mathfrak{f}_{\chi} = \mathfrak{f}_{\lambda_0^*} = \Delta^{\lambda_0(1)}{}_{\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}}\, N_{\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}}\, \mathfrak{f}_{\lambda_0}.$$

From [1] we know that $\mathfrak{f}_{\chi_p} = \Delta_{\mathbf{Q}(\sqrt[p]{a})/\mathbf{Q}}$.
Moreover

$$\mathfrak{f}_{\chi} = \Delta_{\mathbf{Q}(\eta)/\mathbf{Q}}\, N_{\mathbf{Q}(\eta)/\mathbf{Q}}\, \mathfrak{f}_{\psi}.$$

Therefore, when $a \equiv a^p \pmod{p^2}$, then $p^{p-2} | \mathfrak{f}_{\chi_p} = \Delta_{\mathbf{Q}(\sqrt[p]{a})/\mathbf{Q}}$. See [1]. Also

$$\Delta_{\mathbf{Q}(\sqrt[p^2]{a})/\mathbf{Q}} = \Delta^p{}_{\mathbf{Q}(\sqrt[p]{a})/\mathbf{Q}}\, N_{\mathbf{Q}(\sqrt[p]{a})\mathbf{Q}}\, \Delta \quad [\Delta = \Delta_{\mathbf{Q}(\sqrt[p^2]{a}/\mathbf{Q}(\sqrt[p]{a})}].$$

Hence, when $a \equiv a^p \pmod{p^2}$

$$p^{p-2}\, \Delta_{\mathbf{Q}(\eta)/\mathbf{Q}}\, N_{\mathbf{Q}(\eta)/\mathbf{Q}}\, \mathfrak{f}_\psi = p^{(p-2)p}\, N_{\mathbf{Q}(\sqrt[p]{a})/\mathbf{Q}}\, \Delta$$
$$\Rightarrow p^{p-2+2p^2-3p}\, N_{\mathbf{Q}(\eta)/\mathbf{Q}}\, \mathfrak{f}_\psi = p^{(p-2)p}\, N_{\mathbf{Q}(\sqrt[p]{a})/\mathbf{Q}}\, \Delta$$
$$\Rightarrow p^{p^2-2}\, N_{\mathbf{Q}(\eta)/\mathbf{Q}}\, \mathfrak{f}_\psi = N_{\mathbf{Q}(\sqrt[p]{a})/\mathbf{Q}}\, \Delta.$$

Since $N_{\mathbf{Q}(\eta)/\mathbf{Q}}\, \mathfrak{f}_\psi$ is an integral ideal of $\mathbf{Z}$, the proof of the lemma 1 is complete.

Department of Mathematics,
Catholic University,
Toernooiveld, Nijmegen, The Netherlands

REFERENCES

1. WAALL, R. W. VAN DER, On the conductor of the non-abelian simple character of the Galois group of a special field extension, Symposia Mathematica of INDAM, to appear.
2. BERWICK, W. E. H., Integral Bases, Nr. 22 Cambridge Tracts in Mathematics and Mathematical Physics, Cambridge University Press, London, 1927.
3. TSCHEBOTARÖW, N., Grundzüge der Galois'schen Theorie, Noordhoff, Groningen-Djakarta, 1950.